



## Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at <http://about.jstor.org/participate-jstor/individuals/early-journal-content>.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

## *On Certain Ternary Cubic-Form Equations.*

BY J. J. SYLVESTER.

CHAPTER I. *On the Resolution of Numbers into the sums or differences of Two Cubes.*

### SECTION 1.

M. LUCAS has written to inform me that in some one or more of a series of memoirs commencing with 1870, or elsewhere, the Reverend Father Pépin has made considerable additions to my published theorems on the classes of numbers irresoluble into the *sum or difference*\* of two rational cubes.

Using  $p, q$  to denote primes of the forms  $18n + 5$ ,  $18n + 11$ , besides the 6 forms published by me, M. Pépin has found 10 other general classes of irresoluble numbers, the total number (as I understand from M. Lucas) known to the Reverend Father being as follows:

$$\begin{array}{llllll} p, & q^2, & p^2, & q, & 2p, & 2q^2, 4p^2, 4q, \\ 9p, & 9q^2, & 9p^2, & 9q, & 25p, & 25q^2, 5p^2, 5q, \end{array}$$

but the last four of these classes are special cases only, of three out of the four more general irresoluble classes  $pq$ ,  $p^2q^2$ ,  $p_1p_2^2$ ,  $q_1q_2^2$ , where  $p_1, p_2$  are any two numbers of the  $p$  class and  $q_1, q_2$  any two of the  $q$  class. On making  $p = 5$  in the first two of these, and  $p_1 = 5$ ,  $p_2 = p$ , or  $p_2 = 5$ ,  $p_1 = p$ , in the third, Father Pépin's last four classes result. It is also true that the numbers in my four additional general classes respectively multiplied by 9 are still irresoluble. Hence the number of known classes of numbers (depending on  $p$  and  $q$ ) irresoluble into the sum or difference of cubes may be arranged as follows:

$$\begin{array}{llllll} p, & q, & p^2, & q^2, & pq, & p^2q^2, p_1p_2^2, q_1q_2^2, \\ 9p, & 9q, & 9p^2, & 9q^2, & 9pq, & 9p^2q^2, 9p_1p_2^2, 9q_1q_2^2, \\ 2p, & 4q, & 4p^2, & 2q^2. \end{array}$$

Moreover, I have ascertained the truth of the following two theorems of a somewhat different character :

1°. Let  $\rho, \psi, \phi$  denote prime numbers respectively of the forms  $18n + 1$ ,  $18n + 7$ ,  $18n + 13$  and suppose  $\rho, \psi, \phi$  to be *not* of the form  $f^2 + 27g^2$  and

---

\* It is well to understand that a number resoluble into the sum is necessarily also resoluble into the difference of two positive cubes and *vice versa*.

consequently *not* to possess the cubic residue 2, then I say that all the numbers comprised in any one of the eight classes

$$2\rho, \ 4\rho, \ 2\rho^2, \ 4\rho^2, \ 2\psi, \ 4\psi, \ 4\phi, \ 2\phi^2$$

are irresoluble into the sum of two cubes.\*

2°. Provided 3 is not a cubic residue to  $\nu$ † [where  $\nu$ , any  $6n+1$  prime, is the same as  $\rho, \phi, \psi$  taken collectively],  $3\nu$  and  $3\nu^2$  are similarly irresoluble.

With the aid of these theorems and certain special cases of irresolvability noticed by Father Pépin, communicated to me by M. Lucas, supplemented by calculations of M. Lucas and my own as regards the non-excluded numbers, it follows (*mirabile dictu*) that of the first 100 of the natural order of numbers, there is only a single one, viz. 66, of which it cannot at present be affirmed with certitude either that it is or is not resolvable into the sum of two cubes, and of which, in the former case, the resolution cannot be exhibited.

The proof of these statements, and the resolutions into cubes in their lowest terms, when they exist, will be given in the next number of the Journal. For the present I limit myself to noticing (what I much regret not to have done before the paper was printed) a statement of M. Lucas which is capable of being misunderstood and might give rise to an erroneous conception.

It is where this distinguished contributor to our Journal speaks of deriving from one rational point on a cubic curve (defined by a cubic equation with integer coefficients) another by means of its intersections with a conic drawn through five consecutive points situated at the given rational one; but, in fact, it follows from my theory of *residuation* that this point is

\* The exclusion of 2 as a cubic residue blocks out the possibility of the "distribution of the amplitude;" the form  $p^2 + 27q^2$  blocks out the possibility of a solution in which  $x^2 - xy + y^2$  has a common factor with the amplitude, and thereby imposes upon the equation containing  $x, y, z$  (were it soluble in integers) the necessity of repeating itself perpetually in with smaller numbers, which of course is impossible. But the two conditions thus separately stated are in fact mutually implicative, every number of the form  $f^2 + 27g^2$  having 2 for a cubic residue and *vice versa* every number of the form  $6n+1$  to which 2 is a cubic residue being of the form  $f^2 + 27g^2$ . The sole condition, therefore, in order that a number coming under any of the eight categories in the text shall be known at sight to be irresoluble into the sum of two cubes, is that its variable part shall not be of the form  $p^2 + 27q^2$ , *i. e.* shall not be 31, 43, 91, 109, 127, 157, 223, 229, 247, etc.

† If I am not mistaken this is tantamount to the proviso that  $\nu$  shall not be of the form  $f^2 \pm 9fg + 81g^2$ . It is worth noticing that the above quantity multiplied by 3, say  $3N$ , is equal to  $\frac{(9g \mp f)^3 + (18g \pm f)^3}{27g}$ , so that when  $g$  is a cube number  $N$  is immediately resolvable. The initial values of  $N$  will be found to be 61, 67, 73, 103, 151, 193, 271, 367, 547, etc., for each of which, up to 367 inclusive,  $g = 1$  or  $g = -1$ , so that their products by 3 are immediately resolvable.

collinear with the given point and its second tangential: just as a ninth point in which the cubic would be met by any other cubic passing through *eight* consecutive points situated at the given point would be the third tangential to the latter.\*

Hence M. Lucas' third method amounts only to a combination of the other two; and in fact there is *but one single scale* of rational derivatives from any given point in a general cubic, the successive terms of which expressed in terms of the coordinates of the primitive are of the orders 1, 4, 16, 25, 49, . . . the squares of the natural numbers with the multiples of 3 omitted.†

### *Scholium.*

I term *lmn* the *amplitude* of the equation  $lx^3 + my^3 + nz^3 = 0$ , and if  $A$  cannot be broken up in any way into factors  $l, m, n$ , such that  $lx^3 + my^3 + nz^3 = 0$  shall be soluble in integers, I call the amplitude  $A$  of the equation  $x^3 + y^3 + Az^3 = 0$  *undistributable*.

When  $A$  is of the form  $\frac{x^3 - 3x^2y + y^3}{3z^3}$ , the equation  $x^3 + y^3 + Az^3 = 0$  is always soluble, and when this equation is soluble, then, provided that its amplitude is undistributable and contains no prime factor of the form  $6i + 1$ , the equation  $x^3 - 3x^2y + y^3 = 3Az^3$  must be soluble in integers, which cannot be the case when  $A$  contains any factor other than 3, or of the form  $18i \pm 1$ , inasmuch as *the cubic form*  $x^3 - 3x \pm 1$  *contains no factors other than 3 or of the form*  $18i \pm 1$ .

This last theorem is a particular case of the following: If  $k$  be any integer and  $F(x y)$ , the product of factors of the form  $(x - 2 \cos \frac{\lambda\pi}{k} y)$ , where

\*I make the important additional remark that at those special points of the cubic where this ninth point (sometimes elegantly called the subosculatrix) coincides with the point osculated, the scheme of rational derivatives returns upon itself, and instead of an infinite number there will be only two rational derivatives to such point. That is to say the infinite scheme becomes a system of 3 continually recurring points. The general theory of the special points which have only a finite number of rational derivatives will be given in the next number of the Journal.

†When the cubic is of the form  $Ax^3 + Ay^3 + Cz^3 + Mxyz = 0$ , where  $A, C, M$  are integers, then a rational point of inflection  $x = 1, y = -1, z = 0$  is known and, in that case, from any other rational point *besides the ordinary ones* derivative rational points of the missing orders 9, 36, 81 can be found, but no others, and so universally if in the general cubic a rational point of inflection and a rational point  $(a, b, c)$  are given the scale of rational derivatives will be of the orders 1, 4, 9, 16, . . . in  $a, b, c$ . This scale will of course be duplex, consisting of a series of points and a second series in which the radii drawn through the points of the first series and the point of inflection again meet the cubic.

$\lambda$  is every number prime to  $k$  up to  $\frac{k-1}{2}$ , then  $Fx$  contains no prime factors excepting such as are contained in  $k$  or else are of the form  $ki \pm 1$ .\*

If it could be shown, in analogy with what holds for the quadratic forms  $Fx$  which result from making  $k=8, 10, 12$ , that the cubic form  $x^3 - 3xy^2 \pm y^3$  which results from making  $k=18$  may always be made to represent any prime number of the form  $18n \pm 1$  itself, or else its treble (and for our purpose rational numbers would be as efficient as integers), we should then be able to affirm that any prime  $18n \pm 1$  or else its nonuple could be resolved into the sum of two cubes. As a matter of fact I have ascertained that every prime number  $18n \pm 1$  as far as 537 inclusive (and have no ground for supposing that the law fails at that point) can be represented by  $x^3 - 3xy^2 \pm y^3$  or else by its third part with *integer* values of  $x, y$ . Moreover, I find that the same thing is true of  $17^2, 17 \cdot 19, 19^2, 17 \cdot 37, 19 \cdot 37, 37^2, 17 \cdot 53, 19 \cdot 53, 37 \cdot 53$ , *i. e.* in fact for all the binary combinations of the natural progression of " $r, \rho$ " numbers  $17, 19, 37, 53, 71, 73, 89$  (21 in all), as also  $17^2, 19^2, 37^2$ .† The number of consecutive  $r, \rho$  primes for which the law has been verified, *i. e.* the number of those not exceeding 537 will be found to be 39, viz: 17, 19, 37, 53, 71, 73, 89, 107, 109, 127, 163, 179, 181, 197, 199, 233, 251, 269, 271, 307, 323, 341, 359, 361, 377, 379, 397, 413, 431, 433, 449, 451, 467, 469, 487, 503, 521, 523, 541, which according to the usual canons of induction would, I presume, be considered almost sufficient to establish the theorem for the case of  $k=9$ .

The table of "special cases" of irresoluble numbers found by Father Pépin (according to the information most kindly communicated to me by

\* Thus, by making  $k=8$  we learn that  $x^2 - 2$  contains no factors except 2 and  $8i \pm 1$  and by making  $k=16$ , that  $y^4 - 4y^2 + 2$ , none except 2 or  $16i \pm 1$ , by making  $k=9$  that  $x^3 - 3x + 1$ , by making  $k=18$ , that  $x^3 - 3x - 1$  contain no other factors but 3, or numbers of the form  $18n \pm 1$ . The theorem, I am aware, is well known for the case where  $k$  is a prime number and possibly is so for the general case. The proof of the irresolubility into two cubes of the 20 classes of numbers involving  $p$ 's and  $q$ 's, given at page 280, is an instantaneous consequence of the theorem for the case of  $k=9$ , for which case also there is no shadow of doubt of the theorem being true.

†  $53^2$  has not yet made its appearance. All the primes of that form themselves occurring in the first six hundred numbers have already occurred in my calculations except 557 and 593. I have worked with the formula  $x^3 - 3xy^2 \pm y^3$  [ $x$  and  $y$  relative primes], giving to  $x$  and to  $y$  all the values possible from 1 to 36, and intend to extend the table to the limit of 50 or 100. The longer a moderate-sized number is in making its appearance, the longer it is likely to be before it appears, inasmuch as the large numbers of which it is the residuum or balance are becoming continually greater. It may very well then happen that the missing numbers alluded to may transcend all practicable limits of calculation to find them just as would be the case, for certain values of  $A$ , with finding values of  $x, y$  to satisfy the Pellian equation  $x^2 - Ay^2 = 1$ , were there not a theoretical method of arriving at them.

M. Lucas) comprises the numbers

$$14, 21, 31, 38, 39, 52, 57, 60, 67, 76, 77, 93, 95,*$$

all of which I have verified as irresolute except the number 60, which I accept as such on the erudite and sagacious Father's authority.

Reverting to  $F$ , it is hardly necessary to recall that  $F(x^2 + y^2, xy)$  is the primitive factor of  $x^k - y^k$ , and that it is capable of very easy demonstration that this primitive factor contains no prime factors except such as are divisors of  $k$  or of the form  $ki + 1$ , the linear divisor  $ki - 1$  being here excluded. It seems to be very probable that for  $k = 9$ ,  $F(x, y)$  or else  $3F(x, y)$  does represent any prime of the form  $18n \pm 1$ , and consequently that every such form of prime or else 9 times the same is the sum of two rational cubes. $\dagger$

This last conjectural theorem, it will be noticed, is not in any real analogy to the theorem that every product of primes of the form  $4n + 1$ , and also the double thereof, is the sum of two *integer* squares; the real analogy is between the fact, of which this theorem is a consequence, that  $x^3 - 3xy^2 \pm y^3$  or its third part represents every number which is a product of primes of the form  $18n \pm 1$ , and each one of the facts that  $x^2 - 2y^2$ ,  $x^2 - 5y^2$  represent all numbers of the form  $8i \pm 1$ ,  $10i \pm 1$  respectively, and that  $x^2 - 3y^2$  or its third part represents all numbers of the form  $12i \pm 1$ . On account of its importance to this theory it seems desirable to give a name to the law which governs the prime factors of  $F(x, y)$ , and I take advantage of the circumstance that  $F(x^2 + y^2, xy)$  contains prime factors of the form  $ki + 1$ , but not of the form  $ki - 1$ , whilst  $F(x, y)$  contains prime factors of either of these forms indifferently, to characterize it as the Law of Twin Prime Factors. Let us suppose the circumference of a circle divided by points into  $k$  equal parts, and agree to designate the shorter arc between any two of the points a *primitive* division of the circle in respect to  $k$ , provided that no number less than  $k$  would be adequate to give rise to an equal length of arc, so that  $\frac{2\lambda\pi}{k}$ , when  $\lambda$  is prime to  $k$  and less than  $\frac{k}{2}$ , will serve to represent any such division. The assumed Law of Twin Factors (well known, I repeat, for the case of  $k$  a prime number and possibly in its extended form likewise) may then be enunciated as follows:

\* Of these numbers all except 60, 31, 67, 77, 95 belong to some one or other of the general classes of irresolute numbers given in the text.

$\dagger$  It may be and probably is true also that  $x^3 - 3xy^2 \pm y^3$  will represent the product or else three times the product of any two primes each of which is of the form  $r$  or  $\rho$ , and possibly the square or else three times the square of any  $r$  or  $\rho$ ; it cannot possibly represent three times *any cube*, for if it did we should be able to infer that a cube was resolvable into two cubes, which we know is not true.

*That function of  $x$  whose first coefficient is unity and whose roots are the doubled cosines of all the primitive divisions of the circle in respect to  $k$  contains no prime factors except such as are divisors of, or else when increased or diminished by unity, are divisible by  $k$ .* This may be called again the *Exclusional or Negative Theorem of Twin Factors*; and on the other hand the more extraordinary theorem which asserts (on evidence not yet conclusive) that the function of  $x$  above defined, when made homogeneous in  $x, y$ , will represent (at all events for the case of  $k=9$ ) every prime number of the form  $ki \pm 1$ , or else certain specific multiples of any such number, may be called the *Inclusional or Representational Theorem of Twin Factors*.

---

## ***A New Proof of the Theorem of Reciprocity.***

BY DR. JULIUS PETERSEN, *of Copenhagen, Denmark.*

LET  $a$  and  $b$  be two odd prime numbers,  $a < b$ ; form the equation

$$(2n+1)a - 2mb = r \dots \dots \dots \quad (1)$$

for all the odd numbers  $2n+1$  up to  $p-2$ , and choose  $m$  so that  $r$ , which will be termed a remainder, shall lie between  $-b$  and  $+b$ . The absolute numerical values of these remainders will be all different, and therefore they must be the odd numbers  $1, 3, \dots, (b-2)$ , of which, however, some may be negative. According as the number of these negative values is even or odd we will write

$$\left(\frac{a}{b}\right) = +1 \quad \text{or} \quad \left(\frac{a}{b}\right) = -1.$$

From among the equations (1) we will take out those in which the remainders lie between  $-a$  and  $+a$ ; there is one such equation for every value of  $2m$  up to  $a-1$ ; these equations may be written under the form

$$(a-2m)b - (b-2n-1)a = r, \dots \dots \dots \quad (2)$$

which are evidently the equations for the determination of the sign of  $\left(\frac{b}{a}\right)$ .

Therefore  $\left(\frac{a}{b}\right)$  and  $\left(\frac{b}{a}\right)$  will have the same or opposite signs, according as the number of the remainders between  $-b$  and  $-a$  is even or odd. For such remainders

$$-b < (2n+1)a - 2mb < -a,$$